

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hiroaki SAKAGUCHI

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: INFORMATION PROCESSING APPARATUS AND METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-372521	December 24, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)  
☐ are submitted herewith  
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
Bradley D. Lytle

Registration No. 40,073

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

C. Irvin McClelland  
Registration Number 21,124

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2002年12月24日

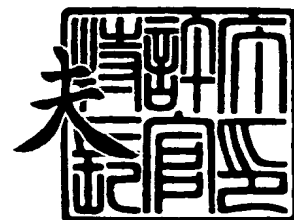
出願番号  
Application Number: 特願2002-372521  
[ST. 10/C]: [JP2002-372521]

出願人  
Applicant(s): ソニー株式会社

2003年 8月19日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2003-3067593



【書類名】 特許願

【整理番号】 0290673106

【提出日】 平成14年12月24日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 坂口 浩章

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法

【特許請求の範囲】

【請求項 1】 複数のデータを結合して圧縮する圧縮手段と、  
前記複数のデータに関する第 1 の付随データを生成する第 1 の生成手段と、  
前記圧縮手段により圧縮されたデータを、前記第 1 の生成手段により生成された前記第 1 の付随データとともに暗号化する暗号化手段と  
を備えることを特徴とする情報処理装置。

【請求項 2】 前記複数のデータは、複数の実行プログラムであることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記第 1 の付随データは、前記複数のデータの個数および大きさに関するデータであることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 前記圧縮されたデータに関する第 2 の付随データを生成する第 2 の生成手段と、  
前記暗号化されたデータ、および、前記第 2 の生成手段により生成された前記第 2 の付随データを格納する格納手段と  
をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】 前記第 2 の付随データは、前記圧縮されたデータの大きさに関するデータであることを特徴とする請求項 4 に記載の情報処理装置。

【請求項 6】 複数のデータを結合して圧縮する圧縮ステップと、  
前記複数のデータに関する付随データを生成する生成ステップと、  
前記圧縮ステップの処理により圧縮されたデータを、前記生成ステップの処理により生成された前記付随データとともに暗号化する暗号化ステップと  
を含むことを特徴とする情報処理方法。

【請求項 7】 暗号化されたデータを復号する復号手段と、  
前記復号手段により、複数のデータが結合されて圧縮されたデータ、および、  
前記複数のデータに関する付随データを復元し、前記複数のデータが結合されて



圧縮されたデータを伸張する伸張手段と

を備えることを特徴とする情報処理装置。

【請求項 8】 前記複数のデータは、複数の実行プログラムであることを特徴とする請求項 7 に記載の情報処理装置。

【請求項 9】 前記付随データは、前記複数のデータの個数および大きさに関するデータである

ことを特徴とする請求項 7 に記載の情報処理装置。

【請求項 10】 前記付随データに基づいて、前記複数のデータの所在に関する管理テーブルを作成する作成手段と、

前記複数のデータ、および前記作成手段により作成された前記管理テーブルを記憶する記憶手段と

をさらに備えることを特徴とする請求項 7 に記載の情報処理装置。

【請求項 11】 暗号化されたデータを復号する復号ステップと、  
前記復号ステップの処理により、複数のデータが結合されて圧縮されたデータ、および、前記複数のデータに関する付随データを復元し、前記複数のデータが結合されて圧縮されたデータを伸張する伸張ステップと

を含むことを特徴とする情報処理方法。

【請求項 12】 複数のデータを結合して圧縮する圧縮手段と、  
前記複数のデータに関する第 1 の付随データを生成する第 1 の生成手段と、  
前記圧縮手段により圧縮されたデータを、前記第 1 の生成手段により生成された前記第 1 の付随データとともに暗号化する暗号化手段と、

前記圧縮されたデータに関する第 2 の付随データを生成する第 2 の生成手段と

、  
前記暗号化されたデータ、および、前記第 2 の付随データを格納する格納手段と、

前記格納手段に格納されている前記暗号化されたデータを復号する復号手段と

、  
前記復号手段により、前記圧縮されたデータ、および、前記第 1 の付随データを復元し、前記圧縮されたデータを伸張する伸張手段と、



前記伸張手段により伸張された前記複数のデータの中から、所定のデータを選択する選択手段と、

前記選択手段により選択された前記所定のデータの処理を実行する実行手段とを備えることを特徴とする情報処理装置。

【請求項 1 3】 前記第 2 の付随データに基づいて、前記複数のデータの所在に関する管理テーブルを作成する作成手段と、

前記伸張手段により伸張された前記複数のデータ、および前記作成手段により作成された前記管理テーブルを記憶する記憶手段と

をさらに備えることを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 1 4】 前記実行手段は、前記記憶手段に記憶されている前記管理テーブルに基づいて、前記所定のデータの処理を実行する

ことを特徴とする請求項 1 3 に記載の情報処理装置。

【請求項 1 5】 前記復号手段による復号処理、および前記伸張手段による伸張処理の開始を指示するとともに、前記復号処理および前記伸張処理の終了を通知する通信手段をさらに備える

ことを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 1 6】 前記複数のデータは、複数の実行プログラムである

ことを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 1 7】 前記第 1 の付随データは、前記複数のデータの個数および大きさに関するデータであり、

前記第 2 の付随データは、前記圧縮されたデータの大きさに関するデータである

ことを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 1 8】 複数のデータを結合して圧縮する圧縮ステップと、

前記複数のデータに関する第 1 の付随データを生成する第 1 の生成ステップと

、  
前記圧縮ステップの処理により圧縮されたデータを、前記第 1 の生成ステップの処理により生成された前記第 1 の付随データとともに暗号化する暗号化ステップと、



前記圧縮されたデータに関する第2の付随データを生成する第2の生成ステップと、

前記暗号化されたデータ、および、前記第2の付随データを格納する格納ステップと、

前記格納ステップの処理により格納された、前記暗号化されたデータを復号する復号ステップと、

前記復号ステップの処理により、前記圧縮されたデータ、および、前記第1の付随データを復元し、前記圧縮されたデータを伸張する伸張ステップと、

前記伸張ステップの処理により伸張された前記複数のデータの中から、所定のデータを選択する選択ステップと、

前記選択ステップの処理により選択された前記所定のデータの処理を実行する実行ステップと

を含むことを特徴とする情報処理方法。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、情報処理装置および方法に関し、特に、例えば、複数の実行プログラムを圧縮し、圧縮されたデータを、各プログラムの付随データとともに暗号化するようにした情報処理装置および方法に関する。

##### 【0002】

##### 【従来の技術】

最近、複数のCPUが混載されたLSI (Large Scale Integrated) が使用されることが多くなっている。また、ソフトウェアソリューション指向のアーキテクチャを採用し、ソフトウェアを入れ替えることで異なるアプリケーションに対応できるLSIが増えつつある。

##### 【0003】

このため、複数のCPUが混載されたLSIや異なるアプリケーションに対応できるLSIを採用した製品には、同じアーキテクチャのインストラクションセットで構成された複数の実行プログラムが必要であり、それらを保存しておくフラッシュ

メモリなどの不揮発性の記憶手段として、より大容量のものが必要とされ、製品コストを高くする要因となっている。

【0 0 0 4】

そこで、例えば、プログラムを圧縮してROMに格納するとともに、圧縮されたプログラムを伸張するためのマップファイルを他のROMに格納することにより、プログラムの容量を削減するようにしている（特許文献 1 参照）。

【0 0 0 5】

また例えば、プログラムの一部を非圧縮状態とし、残りの一部を圧縮してROMに格納することにより、プログラムの容量を削減するようにしているものもある（特許文献 2 参照）。

【0 0 0 6】

また例えば、プログラムを圧縮するとともに、圧縮されたプログラムのヘッダ部分に復元方式に係わる情報を格納しておくことで、プログラムの容量を削減するようにしているものもある（特許文献 3 参照）。

【0 0 0 7】

さらにまた例えば、圧縮されたプログラムと、そのプログラムを展開するための展開プログラムとを一体的にROMに格納することにより、記憶容量を少なくするようにしているものもある（特許文献 4 参照）。

【0 0 0 8】

【特許文献 1】

特開平 1 0 - 1 3 3 8 8 0 号公報

【特許文献 2】

特開平 1 1 - 3 1 2 0 8 9 号公報

【特許文献 3】

特開平 5 - 3 1 3 9 0 4 号公報

【特許文献 4】

特開平 7 - 2 4 8 9 2 1 号公報

【0 0 0 9】

【発明が解決しようとする課題】



このように、プログラムを圧縮することにより記憶容量を削減することができ  
るが、ソフトウェアソリューション指向のアーキテクチャにおいては、重要な技  
術がソフトウェアとして実現されることが多いために、ハードウェアとして実現  
された技術よりも流用しやすく、単にプログラムを圧縮するだけでは、他社によ  
るリバースエンジニアリングが容易になってしまう恐れがあった。

#### 【0010】

そこで、重要な技術を守るため、リバースエンジニアリングが困難であるよう  
なプログラム保存方法がいくつか提案されている。

#### 【0011】

例えば、鍵を用いてプログラムを暗号化する手法があるが、複数のプログラム  
が存在した場合、解読が難しいようにプログラム毎に個別な鍵（例えば、擬似乱  
数の種など）を使用して、個別にプログラムを暗号化することが望ましい。しか  
しながら、個別に暗号化するために、有限な数の鍵を多く消費し、プログラム毎  
に鍵を変える処理が余分に必要となる課題があった。

#### 【0012】

また例えば、LZ (Lempel Ziv) 法、適応的算術符号化法、または、動的ハフマ  
ン符号化のような、徐々に辞書を構築していくような圧縮技法を用いて個別にプ  
ログラムデータを圧縮する手法も考えられるが、プログラム毎に辞書を再構築す  
る必要があり、まとめて圧縮するよりも圧縮率が悪くなる課題があった。

#### 【0013】

さらにまた例えば、同じインストラクションセットを使用しているプログラム  
においては、統計的な性質が似ており、特に、同じシステム上の同じリソースを  
使用するようなプログラムにおいては、アドレス情報や各種デバイスの設定値情  
報などのデータについても統計的な性質が似ている。この性質を利用して、プ  
ログラムをまとめて圧縮することにより、辞書が有効利用できることが望ましい。  
しかしながら、複数のプログラムをまとめて圧縮し、さらに、圧縮された複数の  
プログラムを暗号化するような手法は存在しなかった。

#### 【0014】

本発明はこのような状況に鑑みてなされたものであり、複数のプログラムをま

とめて圧縮し、かつ、圧縮された複数のプログラムを暗号化することにより、プログラムの記憶容量の削減、およびリバースエンジニアリングを防止することができるようにするものである。

#### 【0015】

##### 【課題を解決するための手段】

本発明の第1の情報処理装置は、複数のデータを結合して圧縮する圧縮手段と、複数のデータに関する第1の付随データを生成する第1の生成手段と、圧縮手段により圧縮されたデータを、第1の生成手段により生成された第1の付随データとともに暗号化する暗号化手段とを備えることを特徴とする。

#### 【0016】

前記複数のデータは、複数の実行プログラムであるものとすることができる。

#### 【0017】

前記第1の付随データは、複数のデータの個数および大きさに関するデータであるものとすることができる。

#### 【0018】

前記圧縮されたデータに関する第2の付随データを生成する第2の生成手段と、暗号化されたデータ、および、第2の生成手段により生成された第2の付随データを格納する格納手段とをさらに設けるようにすることができる。

#### 【0019】

前記第2の付随データは、圧縮されたデータの大きさに関するデータであるものとすることができる。

#### 【0020】

本発明の第1の情報処理方法は、複数のデータを結合して圧縮する圧縮ステップと、複数のデータに関する付随データを生成する生成ステップと、圧縮ステップの処理により圧縮されたデータを、生成ステップの処理により生成された付随データとともに暗号化する暗号化ステップとを含むことを特徴とする。

#### 【0021】

本発明の第1の情報処理装置および方法においては、複数のデータが結合されて圧縮され、複数のデータに関する付随データが生成され、圧縮されたデータが

付随データとともに暗号化される。

【 0 0 2 2 】

本発明の第 2 の情報処理装置は、暗号化されたデータを復号する復号手段と、復号手段により、複数のデータが結合されて圧縮されたデータ、および、複数のデータに関する付随データを復元し、複数のデータが結合されて圧縮されたデータを伸張する伸張手段とを備えることを特徴とする。

【 0 0 2 3 】

前記複数のデータは、複数の実行プログラムであるものとすることができる。

【 0 0 2 4 】

前記付随データは、複数のデータの個数および大きさに関するデータであるものとすることができる。

【 0 0 2 5 】

前記付随データに基づいて、複数のデータの所在に関する管理テーブルを作成する作成手段と、複数のデータ、および作成手段により作成された管理テーブルを記憶する記憶手段とをさらに設けるようにすることができる。

【 0 0 2 6 】

本発明の第 2 の情報処理方法は、暗号化されたデータを復号する復号ステップと、復号ステップの処理により、複数のデータが結合されて圧縮されたデータ、および、複数のデータに関する付随データを復元し、複数のデータが結合されて圧縮されたデータを伸張する伸張ステップとを含むことを特徴とする。

【 0 0 2 7 】

本発明の第 2 の情報処理装置および方法においては、暗号化されたデータが復号されて、複数のデータが結合されて圧縮されたデータ、および、複数のデータに関する付随データが復元され、複数のデータが結合されて圧縮されたデータが伸張される。

【 0 0 2 8 】

本発明の第 3 の情報処理装置は、複数のデータを結合して圧縮する圧縮手段と、複数のデータに関する第 1 の付随データを生成する第 1 の生成手段と、圧縮手段により圧縮されたデータを、第 1 の生成手段により生成された第 1 の付随デー

タとともに暗号化する暗号化手段と、圧縮されたデータに関する第 2 の付随データを生成する第 2 の生成手段と、暗号化されたデータ、および、第 2 の付随データを格納する格納手段と、格納手段に格納されている暗号化されたデータを復号する復号手段と、復号手段により、圧縮されたデータ、および、第 1 の付随データを復元し、圧縮されたデータを伸張する伸張手段と、伸張手段により伸張された複数のデータの中から、所定のデータを選択する選択手段と、選択手段により選択された所定のデータの処理を実行する実行手段とを備えることを特徴とする。

#### 【 0 0 2 9 】

前記第 2 の付随データに基づいて、複数のデータの所在に関する管理テーブルを作成する作成手段と、伸張手段により伸張された複数のデータ、および作成手段により作成された管理テーブルを記憶する記憶手段とをさらに設けるようにすることができる。

#### 【 0 0 3 0 】

前記実行手段には、記憶手段に記憶されている管理テーブルに基づいて、所定のデータの処理を実行させるようにすることができる。

#### 【 0 0 3 1 】

前記復号手段による復号処理、および伸張手段による伸張処理の開始を指示するとともに、復号処理および伸張処理の終了を通知する通信手段をさらに設けるようにすることができる。

#### 【 0 0 3 2 】

前記複数のデータは、複数の実行プログラムであるものとすることができる。

#### 【 0 0 3 3 】

前記第 1 の付随データは、複数のデータの個数および大きさに関するデータであり、第 2 の付随データは、圧縮されたデータの大きさに関するデータであるものとすることができる。

#### 【 0 0 3 4 】

本発明の第 3 の情報処理方法は、複数のデータを結合して圧縮する圧縮ステップと、複数のデータに関する第 1 の付随データを生成する第 1 の生成ステップと

、圧縮ステップの処理により圧縮されたデータを、第1の生成ステップの処理により生成された第1の付随データとともに暗号化する暗号化ステップと、圧縮されたデータに関する第2の付随データを生成する第2の生成ステップと、暗号化されたデータ、および、第2の付随データを格納する格納ステップと、格納ステップの処理により格納された、暗号化されたデータを復号する復号ステップと、復号ステップの処理により、圧縮されたデータ、および、第1の付随データを復元し、圧縮されたデータを伸張する伸張ステップと、伸張ステップの処理により伸張された複数のデータの中から、所定のデータを選択する選択ステップと、選択ステップの処理により選択された所定のデータの処理を実行する実行ステップとを含むことを特徴とする。

#### 【0035】

本発明の第3の情報処理装置および方法においては、複数のデータが結合されて圧縮され、複数のデータに関する第1の付随データが生成され、圧縮されたデータとともに暗号化され、圧縮されたデータに関する第2の付随データが生成され、暗号化されたデータとともに格納される。また、暗号化されたデータが復号されて、圧縮されたデータ、および、第1の付随データが復元され、圧縮されたデータが伸張され、伸張された複数のデータの中から、所定のデータが選択され、処理が実行される。

#### 【0036】

##### 【発明の実施の形態】

以下、図を参照して、本発明の実施の形態について説明する。

#### 【0037】

図1は、本発明を適用したマイクロコンピュータの構成例を示す図である。CPU (Central Processing Unit) 1は、不揮発性メモリ2からRAM3に読み出された実行プログラムに従って各種の処理を実行する。

#### 【0038】

不揮発性メモリ2は、例えば、EEPROM (Electrically Erasable and Programmable Read Only Memory) やフラッシュメモリなどで構成され、圧縮および暗号化された、CPU1が各種の処理を実行する上において必要な実行プログラムなど

を記憶する。

#### 【0039】

RAM 3 は、例えば、DRAM (Dynamic Random Access Memory) やSRAM (Static RAM) などの読み書き可能なメモリで構成され、不揮発性メモリ 2 から読み出された実行プログラムを保存する他、その実行プログラムの開始アドレスなどを管理するプログラム管理テーブル 51 (図 3) も保存する。

#### 【0040】

CPU 1、不揮発性メモリ 2、およびRAM 3は、バス 4 を介して相互に接続されている。

#### 【0041】

図 2 は、不揮発性メモリ 2 に格納されるデータの構造例を表わしている。同図に示されるように、予め決められた順番に実行プログラム A 乃至 D が結合されたものがデータ 21 とされ、不揮発性メモリ 2 に格納されている。

#### 【0042】

CPU 1 は、データ 21 に含まれる実行プログラムの個数 (図 2 の例の場合、4 個) を表わす情報データ 22 を生成するとともに、データ 21 に含まれる各実行プログラムのサイズ (図 2 の例の場合、S1 乃至 S4) を表わす情報データ 23 を生成する。

#### 【0043】

この情報データ 23 により、複数の実行プログラム A 乃至 D が結合されたデータ 21 が不揮発性メモリ 2 から RAM 3 に読み出されても、CPU 1 は、データ 21 内での相対的なアドレスを算出することができるため、各実行プログラムの開始アドレスを容易に知ることができる。

#### 【0044】

CPU 1 は、LZ77 法などの慣用圧縮技法を用いて、複数の実行プログラム A 乃至 D が結合されたデータ 21 を圧縮し、プログラムデータ 24 を生成するとともに、圧縮されたプログラムデータ 24 のサイズ (図 2 の例の場合、S5) を表わす情報データ 25 を生成する。

#### 【0045】

さらにCPU1は、圧縮されたプログラムデータ24、情報データ（個数データ）22、および情報データ（サイズデータ）23の3つのデータを連結して1つのデータとして、それを擬似乱数と1方向性関数を使ったワнтаイムパッド暗号などの慣用暗号化技法を用いて暗号化し、データ26を生成する。ここで、プログラムデータ24とデータ26のデータサイズがほぼ同じになるように暗号化される。そして、暗号化されたデータ26、および圧縮されたプログラムデータ24のサイズを表わす情報データ25が、不揮発性メモリ2に格納される。

#### 【0046】

図3は、不揮発性メモリ2に格納されている、暗号化されたデータ26がCPU1により伸張され、実行プログラムとしてRAM3に保存され、実行されるまでの処理を模式的に示している。

#### 【0047】

なお、1つのCPUに対して複数のプログラムを対応させることができるものとするため、便宜上、CPU1を、CPU1-1乃至1-3として図示し、CPU1-1では実行プログラムAが実行され、CPU1-2では、実行プログラムBが実行され、CPU1-3では、実行プログラムCまたは実行プログラムDが実行されるものとする。

#### 【0048】

不揮発性メモリ2には、図2を用いて上述したように、暗号化されたデータ26、および圧縮されたプログラムデータ24のサイズを表わす情報データ25が格納されている。

#### 【0049】

例えば、CPU1-1は、不揮発性メモリ2からデータ26および情報データ25を読み出し、暗号化されたデータ26を復号して、プログラムデータ24、情報データ22、および情報データ23を復元する。CPU1-1は、さらに、圧縮されたプログラムデータ24を伸張してデータ21を復元し、RAM3に保存する。ここで、CPU1-1は、情報データ25により表わされているサイズ分のデータについて、全て復号処理および伸張処理したとき、それらの処理を終了した判断する。

**【0 0 5 0】**

復号処理および伸張処理において、ワнтаイムパッド暗号とLZ77法のような逐次処理が可能な方法が組み合わされて用いられている場合には、CPU 1 - 1 は、プログラムデータ 2 4 を保存するためのワークメモリを必要とせずに、復号処理および伸張処理を同時に行いつつ、データ 2 6 からデータ 2 1 へ直接変換することができる。

**【0 0 5 1】**

CPU 1 - 1 はまた、復元された情報データ 2 2 および情報データ 2 3 に基づいて、データ 2 1 に含まれる実行プログラムの数とそれぞれのサイズを知ることができるため、それらの情報から各実行プログラムの先頭アドレスをそれぞれ算出し、各実行プログラムと、先頭アドレスおよびサイズの対応付けに関するプログラム管理テーブル 5 1 を作成し、RAM 3 に保存する。

**【0 0 5 2】**

図 3 に示すプログラム管理テーブル 5 1 においては、実行プログラム A と、アドレス 0 1 およびサイズ 0 1 が対応付けられ、実行プログラム B と、アドレス 0 2 およびサイズ 0 2 が対応付けられ、実行プログラム C と、アドレス 0 3 およびサイズ 0 3 が対応付けられ、実行プログラム D と、アドレス 0 4 およびサイズ 0 4 が対応付けられている。

**【0 0 5 3】**

このようにして、RAM 3 内において、プログラム管理テーブル 5 1 により、データ 2 1 に含まれる各実行プログラム A 乃至 D が管理される。

**【0 0 5 4】**

例えば、予め決められた CPU 1、または図示せぬ外部装置より指示された CPU 1 (図 3 の例の場合、CPU 1 - 1) は、RAM 3 に復元されたデータ 2 1、および、プログラム管理テーブル 5 1 に基づいて、予め決められた実行プログラム、または、外部装置より指示された実行プログラムを実行可能な状態にして、それを実行する。

**【0 0 5 5】**

より具体的には、CPU 1 - 1 は、RAM 3 で管理されているプログラム管理テーブ



ル 5 1 から、実行すべきプログラム（いまの場合、実行プログラム A）に対応付けられている先頭アドレス（いまの場合、アドレス 0 1）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出する。開始アドレスは、先頭アドレスからの相対アドレスが予め決められていれば、容易に算出することができる。そして CPU 1 - 1 は、RAM 3 内における、算出された開始アドレスにジャンプし、実行プログラム A の実行を開始する。

#### 【 0 0 5 6 】

また、CPU 1 - 2 は、RAM 3 で管理されているプログラム管理テーブル 5 1 から、実行すべきプログラム（いまの場合、実行プログラム B）に対応付けられている先頭アドレス（いまの場合、アドレス 0 2）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出し、そのアドレスにジャンプして、実行プログラム B の実行を開始する。

#### 【 0 0 5 7 】

同様に、CPU 1 - 3 も、RAM 3 で管理されているプログラム管理テーブル 5 1 から、実行すべきプログラム（いまの場合、実行プログラム C または実行プログラム D）に対応付けられている先頭アドレス（いまの場合、アドレス 0 3 またはアドレス 0 4）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出し、そのアドレスにジャンプして、実行プログラム C または実行プログラム D の実行を開始する。

#### 【 0 0 5 8 】

次に、図 4 のフローチャートを参照して、CPU 1 - 1 が実行する、複数のプログラムの格納処理について説明する。

#### 【 0 0 5 9 】

ステップ S 1 において、CPU 1 - 1 は、予め決められた順番、もしくは、図示せぬ外部装置より指示された順番に、複数の実行プログラムを結合する。これにより、図 2 で示したように、実行プログラム A 乃至 D が結合されたデータ 2 1 が生成される。

#### 【 0 0 6 0 】

ステップ S 2 において、CPU 1 - 1 は、ステップ S 1 の処理で結合されたデー

タ 2 1 に含まれる実行プログラムの個数を計数し、個数（図 2 の例の場合、4 個）を表わすデータとして情報データ 2 2 を生成する。ステップ S 3 において、CPU 1-1 は、ステップ S 1 の処理で結合されたデータ 2 1 に含まれる各実行プログラムのサイズをそれぞれ算出し、サイズ（図 2 の例の場合、S 1 乃至 S 4）を表わすデータとして情報データ 2 3 を生成する。

#### 【0061】

ステップ S 4 において、CPU 1-1 は、ステップ S 1 の処理で結合されたデータ 2 1 を、LZ77 法などの慣用圧縮技法を用いて圧縮し、プログラムデータ 2 4 を生成する。ステップ S 5 において、CPU 1-1 は、ステップ S 4 の処理で圧縮されたプログラムデータ 2 4、ステップ S 2 の処理で生成された情報データ（個数データ）2 2、および、ステップ S 3 の処理で生成された情報データ（サイズデータ）2 3 を連結し、それを擬似乱数と 1 方向性関数を使ったワнтаイムパッド暗号などの慣用暗号化技法を用いて暗号化し、データ 2 6 を生成する。

#### 【0062】

ステップ S 6 において、CPU 1-1 は、ステップ S 4 の処理で圧縮されたデータ 2 4 のサイズを算出し、サイズ（図 2 の例の場合、S 5）を表わすデータとして情報データ 2 5 を生成する。ステップ S 7 において、CPU 1-1 は、ステップ S 5 の処理で暗号化されたデータ 2 6、および、ステップ S 6 の処理で生成された情報データ（サイズデータ）2 5 を不揮発性メモリ 2 に格納する。

#### 【0063】

このように、複数の実行プログラムをまとめて圧縮することで、個別に圧縮する場合に較べてオーバーヘッドが少なく、管理データの削減、および、伸張プログラムや伸張装置を簡素化することができる。

#### 【0064】

また、同一インストラクションセットを用いている実行プログラムは、統計的な性質が似ているため、個別に圧縮するよりも圧縮率の向上が期待できる。さらに、実行プログラムの個数に関する情報（情報データ 2 2）、および、実行プログラムの位置やサイズに関する情報（情報データ 2 3）を、複数の実行プログラムが結合され圧縮されたデータ（プログラムデータ 2 4）と一緒に暗号化するこ

とにより、その暗号化されたデータ（データ 2 6）から、実行プログラムに関する情報を推測するのが難しく、暗号解読をより困難にすることができる。

#### 【0 0 6 5】

次に、図 5 のフローチャートを参照して、CPU 1 - 1 が実行する、不揮発性メモリ 2 に格納された複数のプログラムの伸張処理について説明する。

#### 【0 0 6 6】

ステップ S 2 1 において、CPU 1 - 1 は、不揮発性メモリ 2 から、暗号化されたデータ 2 6、および情報データ（サイズデータ） 2 5 を読み出す。ステップ S 2 2 において、CPU 1 - 1 は、ステップ S 2 1 の処理で読み出された、暗号化されたデータ 2 6 をワнтаイムパッド暗号などで復号し、圧縮されたプログラムデータ 2 4、情報データ（個数データ） 2 2、および情報データ（サイズデータ） 2 3 を復元する。

#### 【0 0 6 7】

ステップ S 2 3 において、CPU 1 - 1 は、ステップ S 2 2 の処理で復元された、圧縮されたプログラムデータ 2 4 を LZ77 法などで伸張し、実行プログラム A 乃至 D が結合されたデータ 2 1 を復元する。ステップ S 2 4 において、CPU 1 - 1 は、ステップ S 2 2 の処理で復元された情報データ（個数データ） 2 2 および情報データ（サイズデータ） 2 3 に基づいて、ステップ S 2 3 の処理で伸張されたデータ 2 1 に含まれる各実行プログラムの先頭アドレスをそれぞれ算出し、各実行プログラムと、先頭アドレスおよびサイズの対応付けに関するプログラム管理テーブル 5 1 を作成する。

#### 【0 0 6 8】

ステップ S 2 5 において、CPU 1 - 1 は、ステップ S 2 3 の処理で復元された、実行プログラム A 乃至 D が結合されたデータ 2 1、および、ステップ S 2 4 の処理で作成されたプログラム管理テーブル 5 1 を RAM 3 に保存する。

#### 【0 0 6 9】

このように、全ての実行プログラムの復号処理および伸張処理を連続して実行することができるため、処理の高速化および簡素化が期待できる。これにより、ソフトウェアでは、デコーダプログラムのサイズ削減につながり、ハードウェア

では、ゲート数の削減につながる。

#### 【0 0 7 0】

また、上述したプログラム伸張処理により、RAM 3 には、複数の実行プログラム A 乃至 D が結合されたデータ 2 1、および、各実行プログラムを管理するためのプログラム管理テーブル 5 1 が保存されるため、CPU 1 は、迅速に、実行すべきプログラムのアドレスにジャンプして、そのプログラムの実行を開始することができる。

#### 【0 0 7 1】

次に、図 6 のフローチャートを参照して、CPU 1 - 1 が実行する、RAM 3 に保存されたプログラムの実行処理について説明する。

#### 【0 0 7 2】

ステップ S 4 1 において、CPU 1 - 1 は、所定のプログラム（例えば、実行プログラム A）の実行が指示されたか否かを判定し、所定のプログラムの実行が指示されるまで待機する。そして、ステップ S 4 1 において、所定のプログラムの実行が指示されたと判定された場合、ステップ S 4 2 に進み、CPU 1 - 1 は、RAM 3 に保存されているプログラム管理テーブル 5 1 に基づいて、実行が指示された所定のプログラム（いまの場合、実行プログラム A）に対応付けられている先頭アドレス（いまの場合、アドレス 0 1）を読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出する。

#### 【0 0 7 3】

ステップ S 4 3 において、CPU 1 - 1 は、RAM 3 内における、ステップ S 4 2 の処理で算出された開始アドレスにジャンプし、所定のプログラム（いまの場合、実行プログラム A）の実行を開始する。ステップ S 4 4 において、CPU 1 - 1 は、所定のプログラムの実行が終了したか否かを判定し、まだプログラム実行中であると判定した場合、ステップ S 4 5 に進む。

#### 【0 0 7 4】

ステップ S 4 5 において、CPU 1 - 1 はさらに、図示せぬ外部装置より、実行中のプログラムの強制終了が指示されたか否かを判定し、強制終了が指示されていないと判定した場合、ステップ S 4 4 に戻り、上述した処理を繰り返し実行す

る。そして、ステップ S 4 4 において、所定のプログラムの実行が終了した、または、ステップ S 4 5 において、実行中のプログラムの強制終了が指示されたと判定された場合、処理は終了される。

#### 【 0 0 7 5 】

このように、RAM 3 に、複数のプログラムが結合されて保存されていても、CPU 1 は、プログラム管理テーブル 5 1 に基づいて、迅速に、実行すべきプログラムの開始アドレスにジャンプし、そのプログラムを実行することができる。

#### 【 0 0 7 6 】

なお、上述した図 4 乃至図 6 の処理は、CPU 1 - 1 が実行する場合について説明したが、CPU 1 - 2 あるいは CPU 1 - 3 が実行することも勿論可能である。

#### 【 0 0 7 7 】

以上においては、プログラム管理テーブル 5 1 から、実行すべきプログラムに対応付けられている先頭アドレスを読み出し、読み出された先頭アドレスから実行プログラムの開始アドレスを算出し、そのアドレスへジャンプして、実行プログラムの実行を開始するようにしたが、例えば、図 7 に示されるように、実行すべきプログラムが格納されている場所を、CPU 1 が、プログラム管理テーブル 5 1 の対応する実行プログラムの先頭アドレスから特定し、そのプログラムをプログラム実行可能な所定のメモリ領域 6 1 に転送する。そして、実行すべき CPU 1 - 1 乃至 1 - 3 のいずれかが、メモリ領域 6 1 内の所定アドレスへジャンプして、そのプログラムの実行を開始することもできる。ただし、この場合、メモリ領域 6 1 と開始アドレスは予め決められているものとする。

#### 【 0 0 7 8 】

このように、特定のメモリ領域 6 1 として、LSI 内に CPU と混載された SRAM や DRAM などを用いることで、高速なプログラム実行が可能となる。

#### 【 0 0 7 9 】

また以上においては、CPU 1 - 1 が、暗号化されたデータ 2 6 の復号処理、圧縮されたプログラムデータ 2 4 の伸張処理、および、プログラム管理テーブルの作成処理を行うようにしたが、例えば、図 8 に示されるように、専用のハードウェアである復号伸張処理装置 7 1 を新たに設け、そこで、これらの処理を行わせ

るようにしてもよい。

#### 【0080】

この場合、図示せぬ外部装置から、または、CPU 1-1乃至1-3から通信手段72を介して、復号伸張処理装置71に対して、復号処理および伸張処理の実行を指示することにより開始される。ここで、通信手段72としては、専用の信号やバス上のレジスタなどで実現することができる。

#### 【0081】

この指示を受けた復号伸張処理装置71は、図5を用いて上述したような復号処理および伸張処理を実行する。すなわち、復号伸張処理装置71は、不揮発性メモリ2から、暗号化されたデータ26、および情報データ25を読み出し（ステップS21）、暗号化されたデータ26を復号して圧縮されたプログラムデータ24、情報データ22、および情報データ23を復元し（ステップS22）、圧縮されたプログラムデータ24を伸張して実行プログラムA乃至Dが結合されたデータ21を復元し（ステップS23）、情報データ22および情報データ23に基づいて、プログラム管理テーブル51を作成し（ステップS24）、RAM3に保存する（ステップS25）。

#### 【0082】

そして復号伸張処理装置71は、処理が完了した旨を、通信手段72を介してCPU1に通知する。このように、CPU1は、通信手段72により、復号伸張処理装置71の処理内容を知ることができる。また通信手段72を利用することで、例えば、CPU1のリセットが解除されること、復号伸張処理装置71がCPU1へ割り込みを発行すること、または、復号伸張処理装置71のステータスレジスタをCPU1がポーリングすることなどの実装も可能となる。

#### 【0083】

以上のようにしてRAM3に復元されたデータ21およびプログラム管理テーブル51を用いて、CPU1-1乃至1-3は、図示せぬ外部装置からの指示により、または、予め決められたようにして、所定の実行プログラムを実行することができる。ここで、「予め決められたようにして」とは、先に実行されたプログラムの中に、次にどのプログラムをどのようにして実行すべきかが記述されている

場合を含むものとする。

**【 0 0 8 4 】**

以上においては、LSI内にCPU 1 と混載されたSRAMやDRAMなどを用いるようにしたが、LSI内部のSRAMについては、CPU 1 が高速アクセスすることが可能であるが、大容量を搭載することが難しい。そこで、例えば、LSI内部ほど高速アクセスが可能ではないが、大容量であるLSI外部のDRAMにデータ 2 1 を格納しておき、CPU 1 が所定のプログラムを実行する場合に、そのプログラムをLSI外部のDRAMからLSI内部のSRAMへコピーしてから実行を開始するようなシステムも考えられる。

**【 0 0 8 5 】**

このようなシステムでは、特定のメモリ領域に内部SRAMを割り当て、状況に応じて複数のプログラムを入れ替えることで、より多くの機能を高速にLSI内部のSRAMで実行することができる。

**【 0 0 8 6 】**

以上のように、CPUの数以上の実行プログラムをデータ 2 1 に含むことは多分にあり、実行プログラムの数を、LSI内部のCPUの数からは推測することができない。従って、複数の実行プログラムがまとめて圧縮され、さらに暗号化されているデータ 2 6 は、その暗号化および圧縮率が隠蔽され、より強固にリバースエンジニアリングを防止することができる。

**【 0 0 8 7 】**

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。

**【 0 0 8 8 】**

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

**【 0 0 8 9 】**

**【発明の効果】**

以上のように、第1の本発明によれば、データの記憶容量を削減することが可能となる。特に、圧縮および暗号化された複数の実行プログラムの記憶容量を削減するとともに、リバースエンジニアリングを防止することが可能となる。

#### 【0090】

第2の本発明によれば、データ処理の高速化および簡素化を実現することが可能となる。特に、圧縮および暗号化された複数の実行プログラムの復号伸張処理の高速化および簡素化を実現することが可能となる。

#### 【0091】

第3の本発明によれば、データの記憶容量を削減し、データ処理の高速化および簡素化を実現することが可能となる。特に、圧縮および暗号化された複数の実行プログラムの記憶容量を削減するとともに、圧縮および暗号化された複数の実行プログラムの復号伸張処理の高速化および簡素化を実現することが可能となる。

#### 【図面の簡単な説明】

##### 【図1】

本発明を適用したマイクロコンピュータの構成例を示す図である。

##### 【図2】

ROMに格納されるデータの構造例を表わす図である。

##### 【図3】

暗号化されたデータが伸張され実行されるまでの処理を模式的に示す図である。

##### 【図4】

複数のプログラムの格納処理を説明するフローチャートである。

##### 【図5】

複数のプログラムの伸張処理を説明するフローチャートである。

##### 【図6】

プログラムの実行処理を説明するフローチャートである。

##### 【図7】

暗号化されたデータが伸張され実行されるまでの他の処理を模式的に示す図で



ある。

【図 8】

暗号化されたデータが伸張され実行されるまでの他の処理を模式的に示す図である。

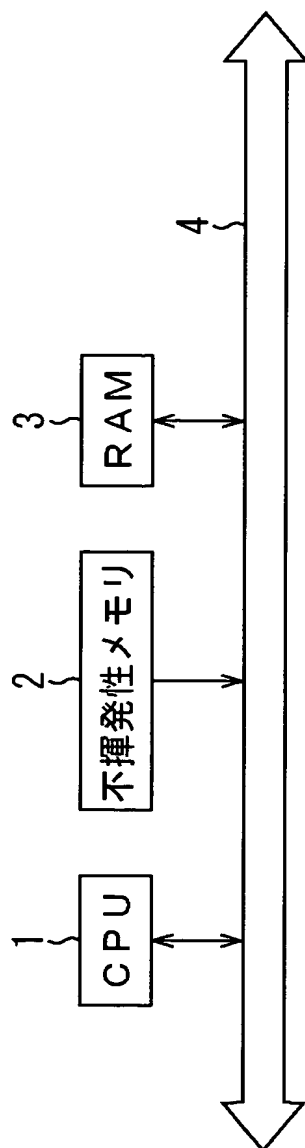
【符号の説明】

1 CPU, 2 不揮発性メモリ, 3 RAM, 7 1 復号伸張装置

【書類名】 図面

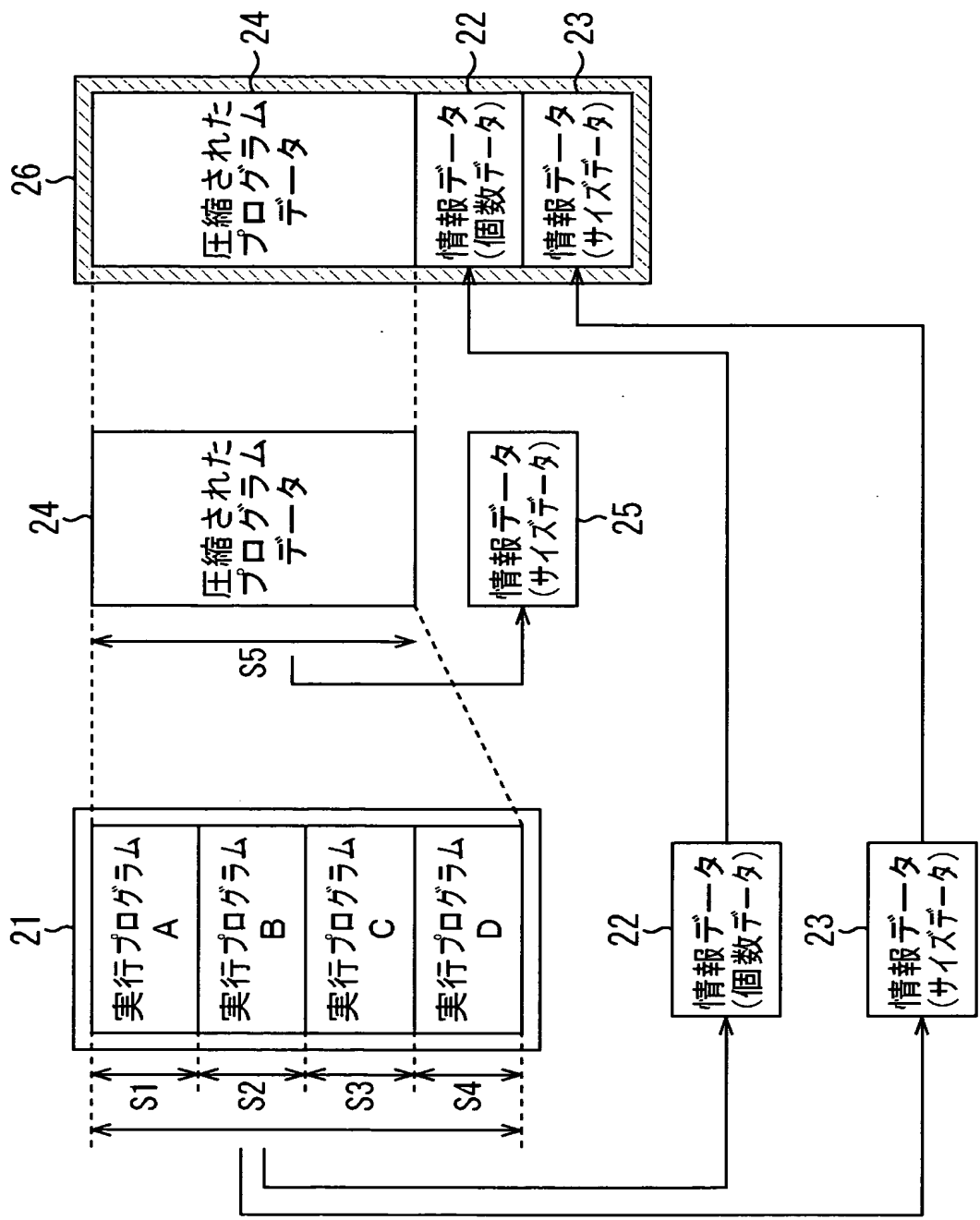
【図 1】

図1



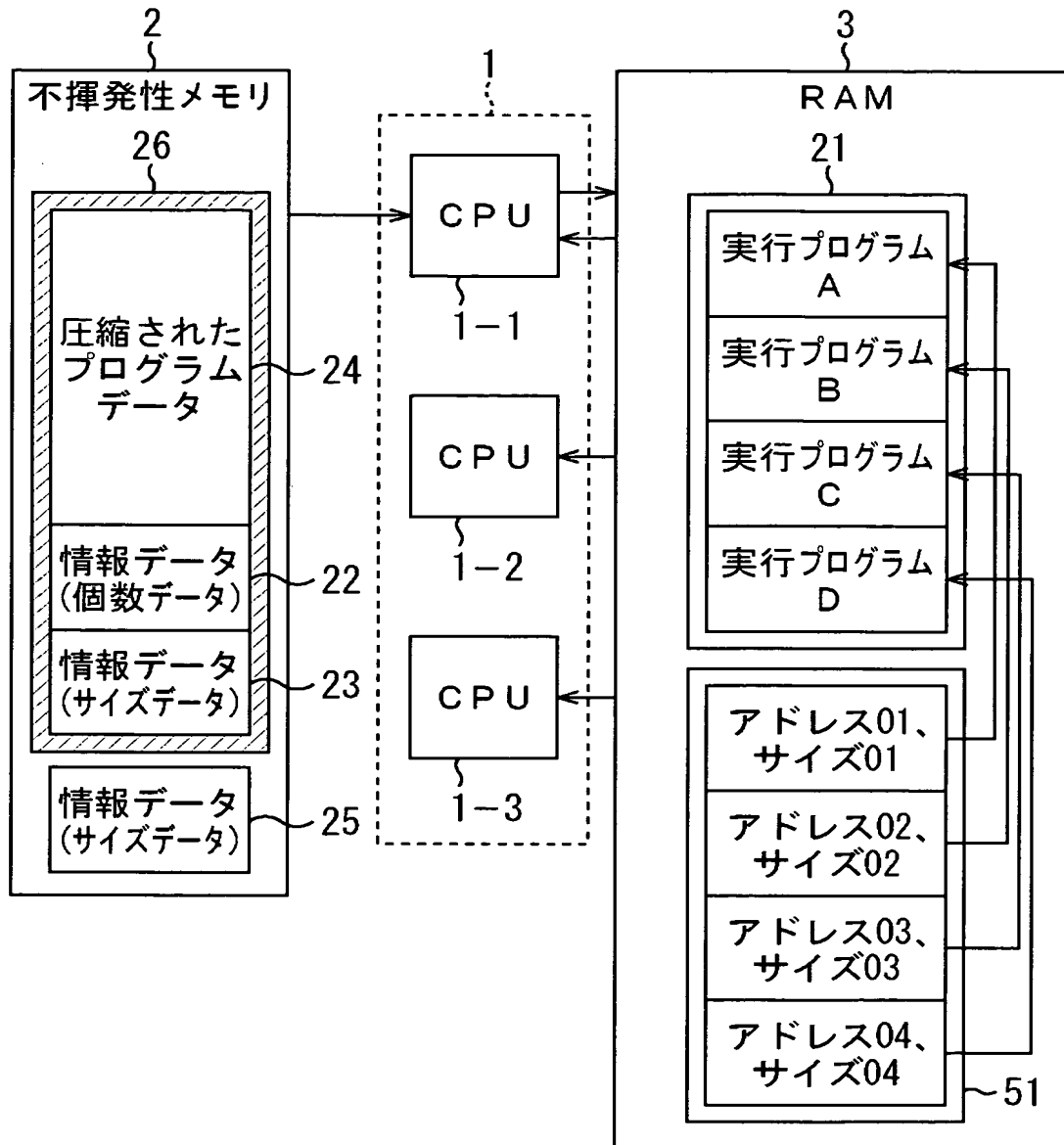
【図 2】

図2



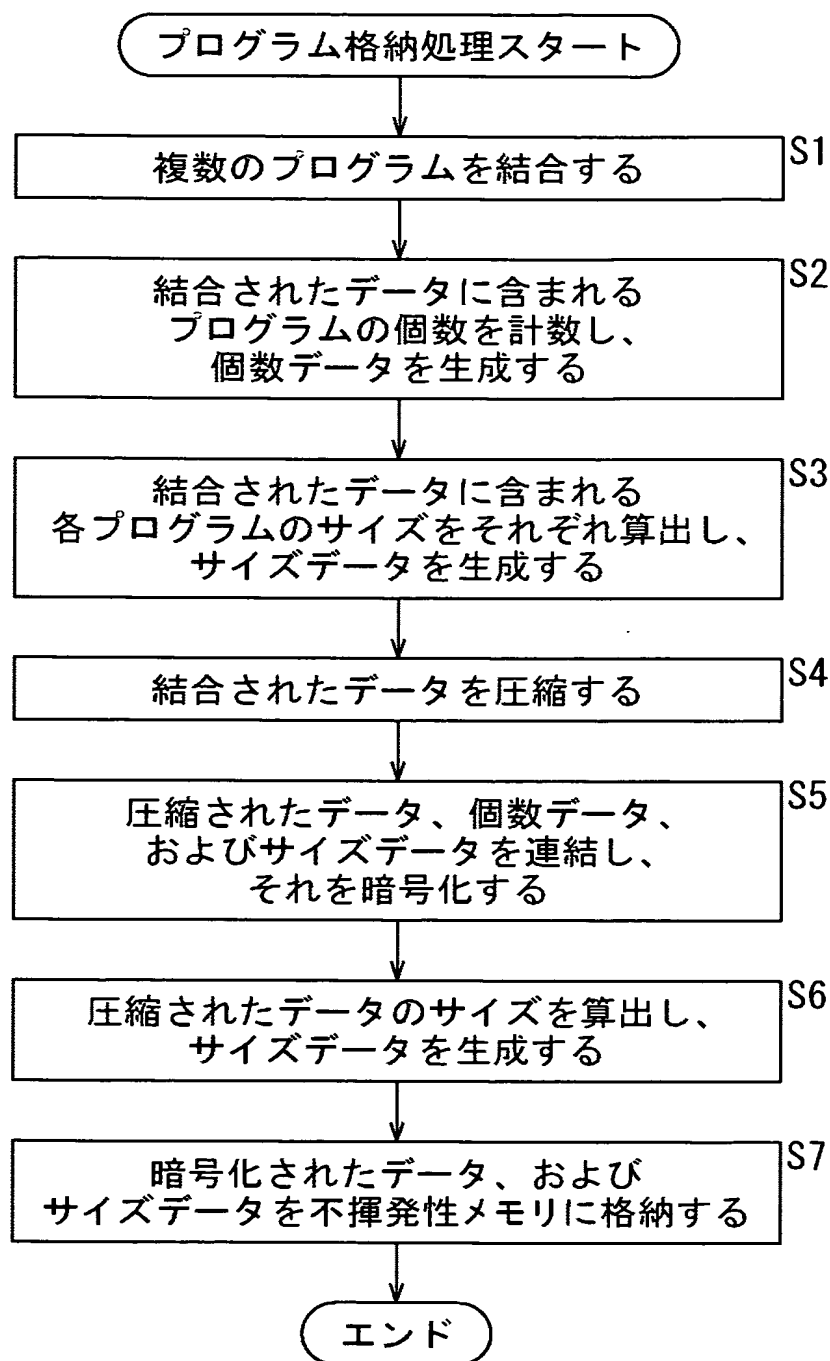
【図3】

図3



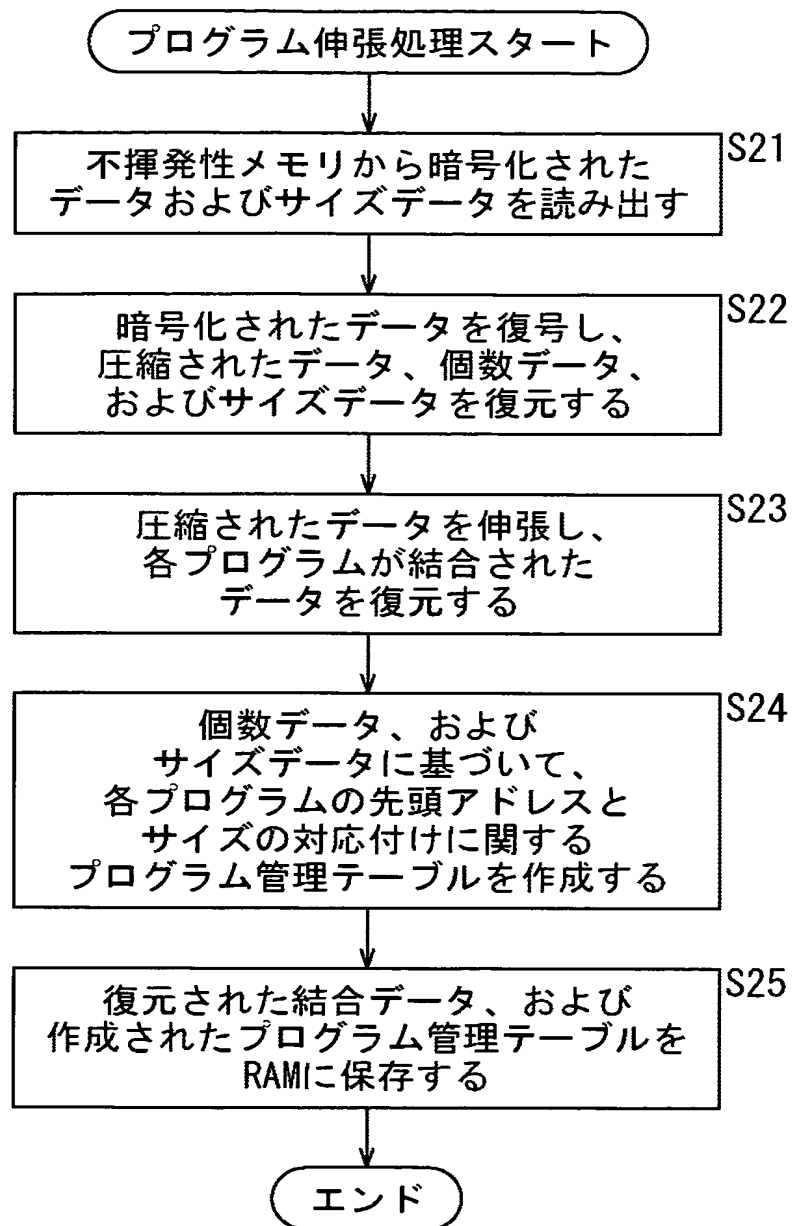
【図 4】

図4



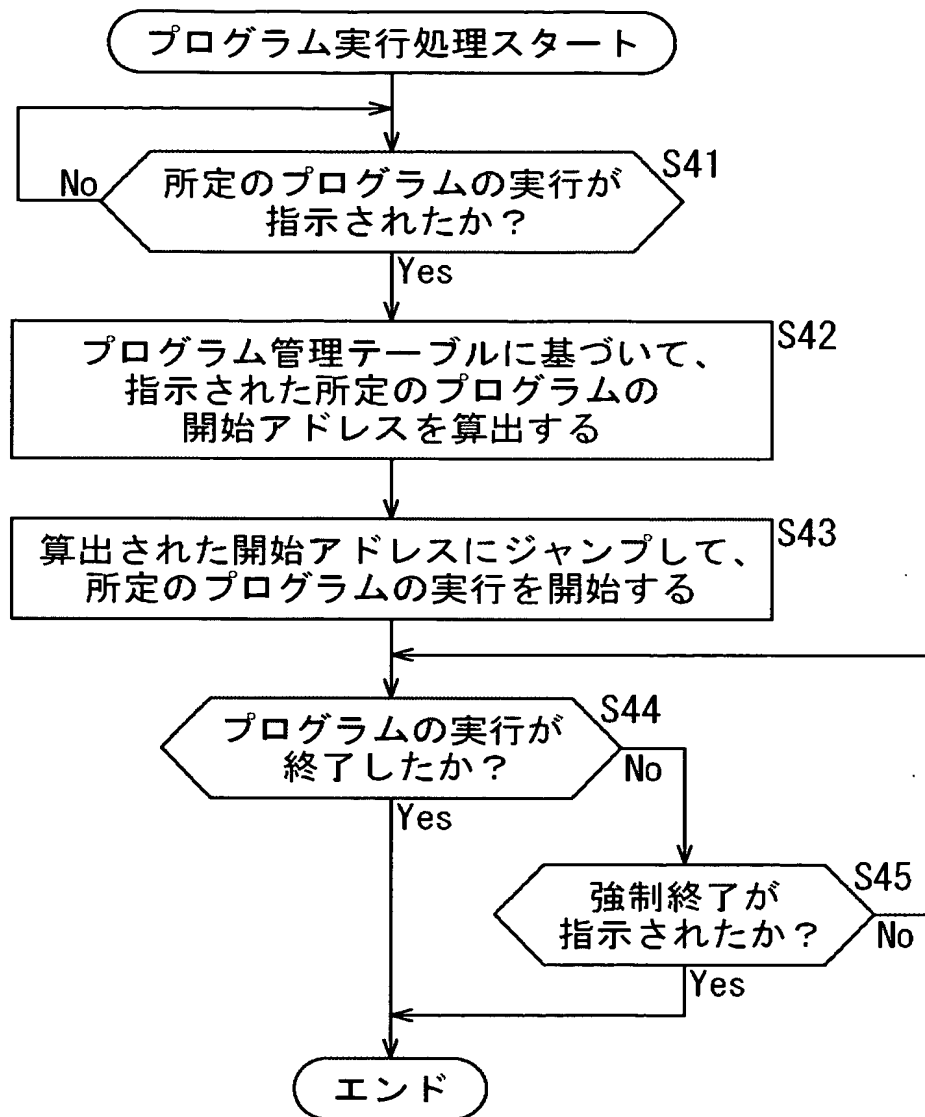
【図 5】

図5



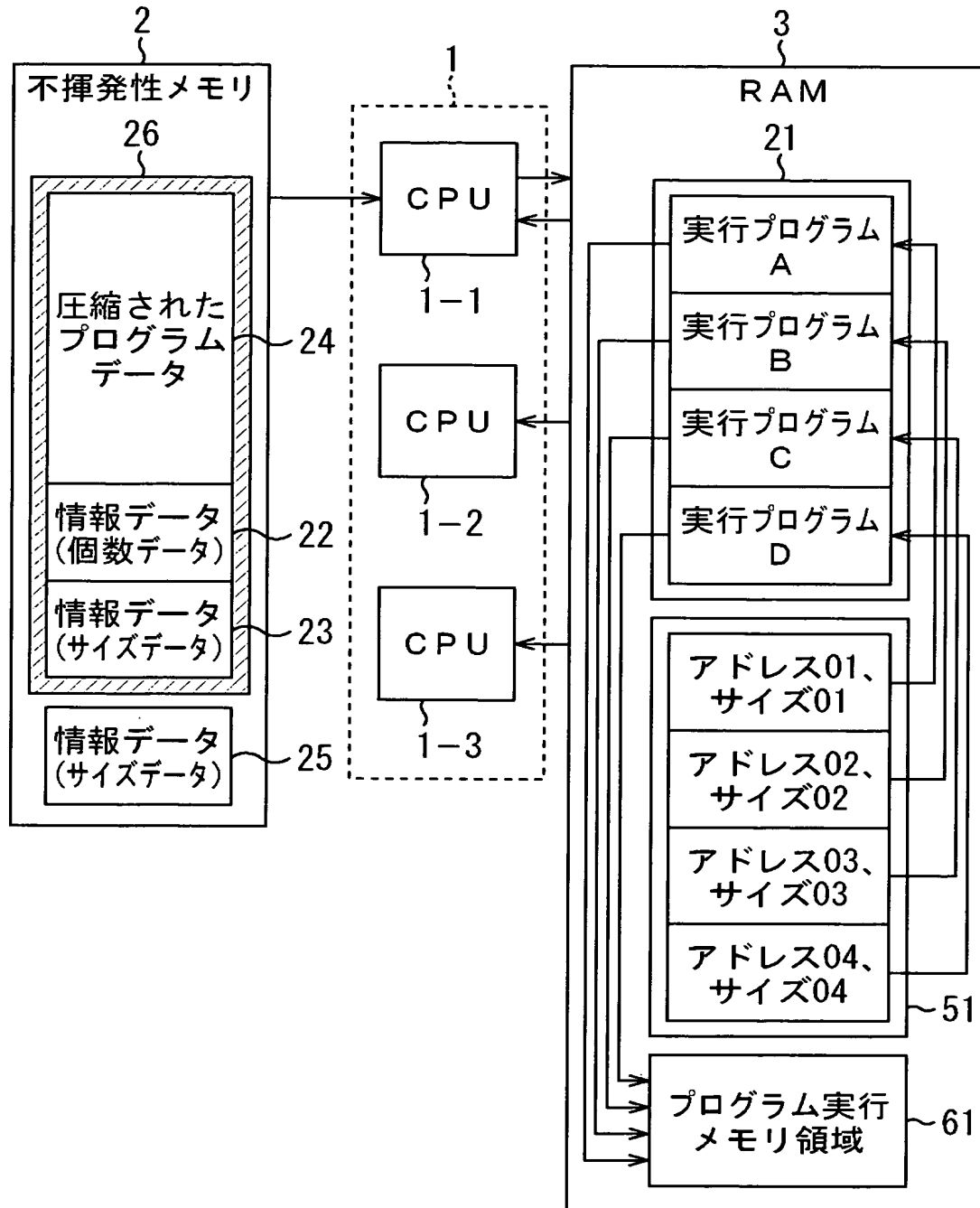
【図 6】

図6



【図7】

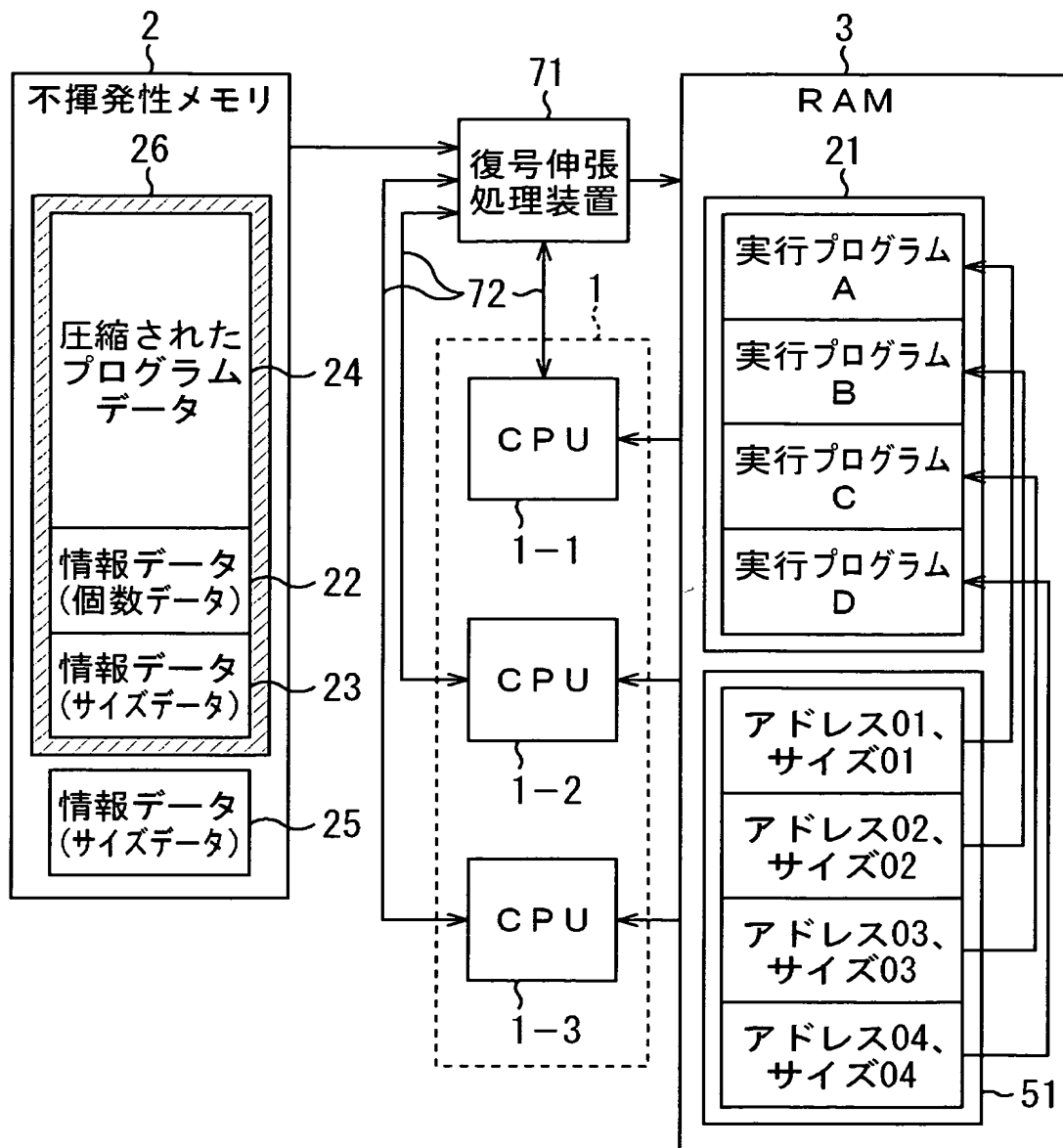
図7





【図 8】

図8



【書類名】 要約書

【要約】

【課題】 プログラムの記憶容量の削減、およびリバースエンジニアリングを防止することができるようにする。

【解決手段】 不揮発性メモリ 2 には、データ 2 1 が圧縮されたプログラムデータ 2 4、データ 2 1 に含まれる実行プログラムの個数を表わす情報データ 2 2、および各実行プログラムのサイズを表わす情報データ 2 3 が連結されて暗号化されたデータ 2 6 が格納されている。CPU 1-1 は、不揮発性メモリ 2 からデータ 2 6 を読み出して復号し、プログラムデータ 2 4、および情報データ 2 2、2 3 を復元した後、プログラムデータ 2 4 を伸張してデータ 2 1 を復元し、RAM 3 に保存する。CPU 1-1 はまた、情報データ 2 2、2 3 に基づいて、各実行プログラムを管理するためのプログラム管理テーブル 5 1 を作成し、RAM 3 に保存する。本発明は、マイクロコンピュータに適用できる。

【選択図】 図 3

特願 2 0 0 2 - 3 7 2 5 2 1

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 1 8 5 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社